ინტერნეტ უსაფრთხოების ინფორმაცია

"პროკრედიტ ბანკი" ვალდებულია უზრუნველყოს თქვენი ტრანზაქციებისა და საბანკო ანგარიშის უსაფრთხოება და ხელშეუხებლობა. აქედან გამომდინარე, თქვენი ონლაინ ტრანზაქციების დაცვის მიზნით "პროკრედიტ ბანკი" უსაფრთხოების უახლეს პროგრამებსა და პროცედურებს იყენებს. მიუხედავად ამისა, ყოველთვის უნდა გახსოვდეთ, რომ ინტერნეტი და ელექტრონული ფოსტა შეიძლება გამოყენებულ იქნას არაკანონიერი საქმიანობისთვის, ამიტომ გირჩევთ მიიღოთ შემდეგი უსაფრთხოების ზომები.

ინტერნეტ უსაფრთხოების რჩევები

უნდა იცოდეთ, ვისთან გაქვთ საქმე

იმისათვის, რომ ინტერნეტ ბანკინგში შეხვიდეთ, ვებ ბრაუზერში ყოველთვის აკრიფეთ ბანკის მისამართი https://online.procreditbank.ge. არ გადახვიდეთ ვებ–გვერდზე ელექტრონულ წერილში მითითებული ბმულის საშუალებით და ნუ მიუთითებთ პირად ინფორმაციას. ეჭვის გაჩენის შემთხვევაში, დაუკავშირდით "პროკრედიტ ბანკს" შემდეგ მისამართზე: infosec@procreditbank.ge

შეინახეთ პაროლები და პინ – კოდი უსაფრთხო ადგილას

სიფრთხილით მოეკიდეთ ყველა უცნობ ელექტრონულ წერილს ან სატელეფონო ზარს თქვენი პირადი მონაცემების ან ბარათის ნომრის გამჟღავნების მოთხოვნით. ეს ინფორმაცია საიდუმლოდ უნდა შეინახოთ. არ გაანდოთ პირადი მონაცემები უცნობ პირებს. თქვენი ბანკი და პოლიცია არასდროს დაგიკავშირდებათ თქვენი პინ–კოდის ან პაროლის გამჟღავნების მოთხოვნით.

გაუფრთხილდით ფულს!

ნუ მოტყუვდებით თითქოსდა გულწრფელი წერილებით, რომლებიც ფულის ადვილად შოვნის შანსს გთავაზობენ. თუ რაიმე შემოთავაზება ზედმეტად კარგი გეჩვენებათ სიმართლისთვის, შესაძლოა ეგრეც იყოს!
განსაკუთრებული სიფრთხილით მოეკიდეთ ქვეყნის გარედან შემოსულ უცნობ წერილებს, ვინაიდან რთულია იმის დადგენა ნამდვილად გაგზავნილია თუ არა ეს წერილები იმ პირების მიერ, რომლებადაც მათ თავი წარადგინეს.

იზრუნეთ თქვენი კომპიუტერის უსაფრთხოებაზე

გამოიყენეთ განახლებული ანტივირუსი და პერსონალური Firewall-ი. თუ თქვენ კომპიუტერში Microsoft Windows-ის საოპერაციო სისტემაა დაყენებული, განაახლეთ ეს პროგრამა Microsoft-ის ვებ–გვერდიდან. ყოველთვის გამოიყენეთ ინტერნეტ ბრაუზერის უახლესი ვერსია, რომელიც ყველა უსაფრთხოების განახლებას შეიცავს. განსაკუთრებით ფრთხილად იყავით ინტერნეტ კაფეებში, ბიბლიოთეკებში ან სხვა, არა თქვენ პერსონალურ კომპიუტერზე მუშაობის დროს.

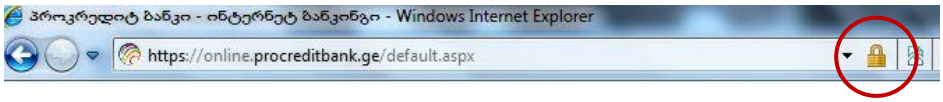
დამატებითი ინფორმაციის მისაღებად შეგიძლიათ ეწვიოთ სპეციალურ ვებ–გვერდებს, მაგალითად: http://www.banksafeonline.org.uk/faq.html

უსაფრთხოების დამატებითი ზომები

- ყოველთვის დაიმახსოვრეთ თქვენი პაროლი და სხვა უსაფრთხოების ზომებთან დაკავშირებული პირადი მონაცემები. რაც შეიძლება მალე გაანადგურეთ ამ ინფორმაციის შემცველი შეტყობინება.
- არ ჩაიწეროთ და არ გადაწეროთ პაროლი და სხვა უსაფრთხოების ზომებთან დაკავშირებული პირადი მონაცემები, გარდა იმ შემთხვევისა, როცა ის სათანადოა დაცული.
- ყოველთვის შეასრულეთ თქვენი ბანკის მითითებები და პირობები.
- მიიღეთ სათანადო ზომები იმისათვის, რომ პაროლი და სხვა უსაფრთხოების ზომებთან დაკავშირებული პირადი მონაცემები ყოველთვის იყოს კონფიდენციალური – არ გაანდოთ ეს ინფორმაცია ოჯახის წევრებს ან მეგობრებს.
- არ გამოიყენოთ ინტერნეტ ბანკინგში შესვლის პაროლი სხვა რაიმე არასაბანკო ვებ–გვერდზე.
- პაროლის შეცვლის შემთხვევაში, აირჩიეთ ისეთი პაროლი, რომლის ადვილად გამოცნობა შეუძლებელია.
- არავის გაანდოთ თქვენი ანგარიშის მონაცემები ან სხვა კონფიდენციალური ინფორმაცია. ბანკთან საუბრისას, ყურადღება მიაქციეთ იმას, თუ რა ინფორმაციას ითხოვენ თქვენგან: როგორც წესი, თქვენ არ მოგთხოვენ სრული პაროლის გამჟღავნებას.
- დარწმუნდით, რომ ყოველთვის იყენებთ **"პროკრედიტ ბანკის" უსაფრთხო ელექტრონულ საბანკო მომსახურებას.** ყოველთვის შედით პირდაპირ ვებ–გვერდზე შემდეგი მისამართის აკრეფით https://online.procreditbank.ge. ბანკის ვებ–გვერდზე შესვლამდე დარწმუნდით, რომ თქვენი ბრაუზერის მარჯვენა ზედა მხარეს ჩაკეტილი. ბოქლომი ან მთლიანი გასაღები არის გამოსახული. უსაფრთო კავშირის დამყარების დროს ბანკის ვებ–გვერდის მისამართი 'http'–დან 'https' –ზე შეიცვლება.
- შეამოწმეთ, ჩანს თუ არა უსაფრთხო კავშირის სიმბოლო (ბოქლომი, ან მთლიანი გასაღები).
- "პროკრედიტ ბანკის" **უსაფრთხოების სერტიფიკატის** გასაცნობად დააწკაპუნეთ ბრაუზერში არსებულ ბოქლომის ნიშანზე.

Internet Explorer 9

Internet Explorer 8



Firefox 4

- ინტერნეტ ბანკინგის გამოყენებასთან დაკავშირებული ჩვეული წესიდან **ნებისმიერი** გადახვევა საეჭვოდ უნდა იქნას მიჩნეული. რაიმე ეჭვის შემთხვევაში, მიმართეთ "პროკრედიტ ბანკს": მიბრძანდით უახლოეს ფილიალში, დაუკავშირდით თქვენს კლიენტთა მრჩეველს ან დარეკეთ ცხელ ხაზზე: (832) 2202222
- ნუ დატოვებთ კომპიუტერს უყურადღებოდ, ინტერნეტ ბანკინგის გახსნილი ვებ–გვერდით.
- ინტერნეტ ბანკინგში მუშაობის დასრულების შემდეგ გამოდით ინტერნეტ ბანკინგიდან ღილაკით "გამოსვლა".

"ფიშინგი"

რა არის "ფიშინგი"?

"ფიშინგი" არის სხვადასხვა შემთხვევით ადრესატებთან ელექტრონული ფოსტის გაგზავნა, რომელიც თითქოსდა გამოგზავნილია ინტერნეტში მოქმედი რეალური ორგანიზაციისგან, რომლის მიზანია მოტყუების გზით აიძულოს ამ ორგანიზაციის კლიენტები გაამჟღავნონ თავიანთი ინფორმაცია თაღლითების მიერ შექმნილ ყალბ ვებ–გვერდზე. ასეთი წერილი, როგორც წესი, იტყობინება, რომ აუცილებელია კლიენტის ანგარიშის "განახლება" ან "გადამოწმება" ელექტრონულ ფოსტაში მოცემული ბმულის საშუალებით, რომელიც ყალბ ვებ–გვერდზე გადადის. ყალბ ვებ–გვერდზე შეყვანილი ნებისმიერი ინფორმაცია თაღლითების ხელში გადადის, რომლებიც მას თავიანთი მიზნებისთვის იყენებენ.

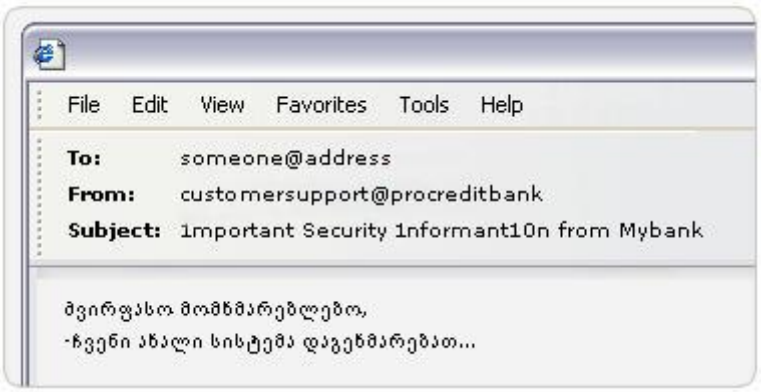
როგორ ავირიდოთ "ფიშინგის" საფრთხე?

მთავარია, სიფრთხილით მოეკიდოთ თქვენს მიერ მიღებულ, ყველა უცნობ და მოულოდნელ ელექტრონულ წერილს, თუნდაც ის ერთი შეხედვით საიმედო წყაროდან იყოსმოწერილი. წერილები შემთხვევით მისამართებზე იგზავნება, რეალურ კლიენტამდე მიღწევის იმედით, რომელსაც სამიზნე ბანკში ანგარიში აქვს გახსნილი.

მართლაც, "პროკრედიტ ბანკი" შეიძლება ელექტრონული ფოსტით დაგიკავშირდეთ, მაგრამ ამ შეტყობინებაში "პროკრედიტ ბანკი" არასდროს მოითხოვს თქვენგან ელექტრონულ ფოსტაში თქვენი პაროლის ან სხვა კონფიდენციალური ინფორმაციის გამჟღავნებას, ბმულზე დაწკაპუნებით ან ვებ–გვერდზე გადასვლის საშუალებით. გახსოვდეთ თუ რა გზით გიკავშირდებათ ხოლმე თქვენი ბანკი და არასდროს გაამჟღავნოთ თქვენი სრული პაროლი ან პირადი ინფორმაცია.

როგორ უნდა ამოიცნოთ თაღლითური "ფიშინგ" წერილი

1 – ვისგან მოვიდა ელექტრონული ფოსტა?



ფიშინგ წერილი შეიძლება გამოიყურებოდეს ისე, თითქოს ის ნამდვილად "პროკრედიტ ბანკის" ელექტრონული ფოსტის მისამართიდანაა მოსული. სამწუხაროდ, ინტერნეტ ფოსტის სტრუქტურის გამო, ფიშერებისათვის შედარებით ადვილია ყალბი ჩანაწერის შექმნა გამომგზავნის ველში.

ელექტრონული მისამართი, რომელიც მითითებულია გამომგზავნის ველში, არ არის იმის გარანტია, რომ წერილი შეტყობინებაში მითითებული პირის ან ორგანიზაციისგანაა მოსული. ასეთი წერილები, შესაძლოა არ იყოს გაგზავნილი საბანკო სისტემიდან.

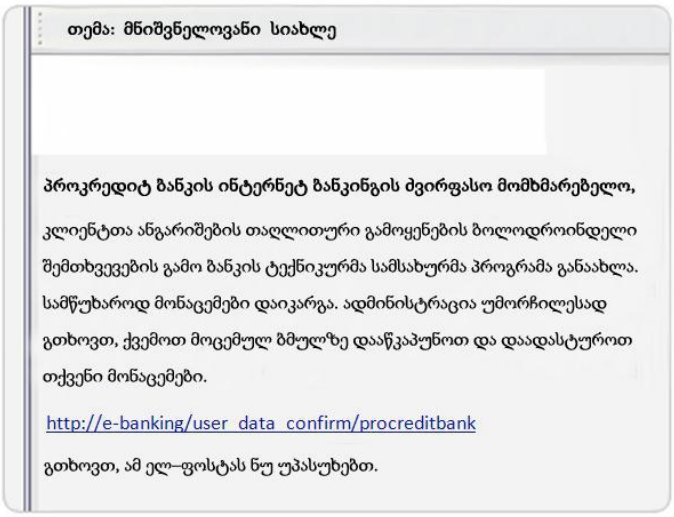
2 – ვისთვისაა განკუთვნილი ელექტრონული ფოსტა?

წერილები იგზავნება საერთო მისამართების სიაში მითითებულ ადრესატებთან. თაღლითებს ნაკლებად ეცოდინებათ თქვენი რეალური სახელი ან რაიმე სხვა ინფორმაცია თქვენს შესახებ, ასე რომ თქვენ ზოგადი სიტყვებით მოგმართავენ, მაგალითად, "ძვირფასო კლიენტო".

3 - ყურადღებით გაეცანით შეტყობინებას - აქვს თუ არა მას "ფიშინგის" ნიშნები?

პირველ რიგში, უნდა გახსოვდეთ, რომ ბანკები არასდროს მოგწერენ ელექტრონულ ფოსტას თქვენი პაროლის ან სხვა კონფიდენციალური ინფორმაციის გამჟღავნების მოთხოვნით. ველში "თემა" სავარაუდოდ იქნება უჩვეულო ან დიდი ზომის ასოები (ეს არის სპამ–ფილტრისგან თავის არიდების მცდელობა), მათ შორის გრამატიკული და ორთოგრაფიული შეცდომები.

თაღლითური შეტყობინების ნიმუში


თემა: მნიშვნელოვანი სიახლე

პროკრედიტ ბანკის ინტერნეტ ბანკინგის ძვირფასო მომხმარებელო,

კლიენტთა ანგარიშების თაღლითური გამოყენების ბოლოდროინდელი შემთხვევების გამო ბანკის ტექნიკურმა სამსახურმა პროგრამა განაახლა. სამწუხაროდ მონაცემები დაიკარგა. ადმინისტრაცია უმორჩილესად გთხოვთ, ქვემოთ მოცემულ ბმულზე დააწკაპუნოთ და დაადასტუროთ თქვენი მონაცემები.

http://e-banking/user_data_confirm/procreditbank

გთხოვთ, ამ ელ–ფოსტას ნუ უპასუხებთ.

არასდროს შეხვიდეთ თქვენ ინტერნეტ ბანკინგში ელექტრონული ფოსტის შეტყობინებაში მითითებულ ბმულზე დაწკაპუნებით.
ყოველთვის გახსენით ვებ ბრაუზერი და თავად შეიყვანეთ "პროკრედიტ ბანკის" ინტერნეტ ბანკინგის მისამართი.

თუ იმ შეტყობინების ნამდვილობასთან დაკავშირებით, რომელიც თითქოსდა "პროკრედიტ ბანკიდან" მოვიდა, რაიმე ეჭვები გაგაჩნიათ, დაუყოვნებლივ შეატყობინეთ "პროკრედიტ ბანკს" უახლოეს ფილიალში მისვლით, თქვენს კლიენტთა მრჩეველთან დაკავშირებით ან შემდეგ ტელეფონის ნომერზე დარეკვით: (832) 2202222. შეგიძლიათ ასევე გადააგზავნოთ საეჭვო შეტყობინება შემდეგ საფოსტო მისამართზე: infosec@procreditbank.ge

4 - სად გაიხსნება ჰიპერბმული?

სამწუხაროდ, ძალიან ადვილია ბმულის რეალური დანიშნულების დამალვა, ასე რომ თქვენი ელექტრონული ფოსტის სტატუსის ველში ჩასმული ბმულის ან ნებისმიერი სხვა ინფორმაციის გაყალბება სირთულეს არ წარმოადგენს.

როგორ უნდა შენიშნოთ თაღლითური ვებგვერდი

რა არის საიტის მისამართი?

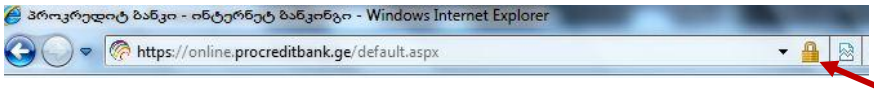
ელექტრონულ ფოსტაში ჩასმულ ბმულზე დაწკაპუნებით ვებ–გვერდზე გადასვლისას, სამისამართო ველიდან ყალბი ვებ–გვერდის რეალური ადგილმდებარეობის დადგენის მრავალი საშუალება არსებობს. ვებ–გვერდის მისამართი შეიძლება იწყებოდეს ნამდვილი გვერდის დომენის სახელით, მაგრამ არ არის იმის გარანტია, რომ ეს გვერდი ნამდვილია. არსებობს სხვა საშუალებებიც: რიცხვების შემცველი მისამართები, მსგავსი მისამართის დარეგისტრირება (როგორიცაა www.mybank-verify.com), ასევე ბრაუზერის ფანჯარაში ყალბი სამისამართო ველის ჩასმა. ამ გვერდებზე ბმულების უმეტესობა შეიძლება ნამდვილ ვებ–გვერდზე გადადიოდეს, ასე რომ არ მოტყუვდეთ.

იმისათვის, რომ დარწმუნდეთ, რომ "პროკრედიტბანკის" ოფიციალურ, უსაფრთხო ვებ–გვერდზე იმყოფებით, შეადარეთ უსაფრთხო კავშირის სიმბოლო.

Internet Explorer 9

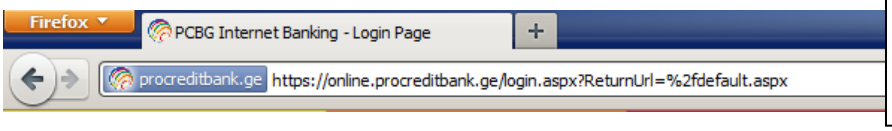
"ბოქლომზე" დაჭერით ვებ–გვერდის უსაფრთხოების იდენტიფიცირების სერტიფიკატი გაიხსნება.

Internet Explorer 8



"ბოქლომზე" დაჭერით ვებ–გვერდის უსაფრთხოების იდენტიფიცირების სერტიფიკატი გაიხსნება.

Firefox 4



თქვენ გაქვთ საშუალება შეამოწმოთ "პროკრედიტ ბანკის" უსაფრთხოების სერტიფიკატი ბრაუზერში არსებულ "ბოქლომის" ნიშანზე დაწკაპუნებით.

მოერიდეთ თაღლითურ pop-up ფანჯრებს

მთლიანად გაყალბებული ვებ–გვერდის გახსნის სანაცვლოდ, თაღლითებს შეუძლიათ ჩატვირთონ ნამდვილი ვებ–გვერდი ბრაუზერის მთავარ ფანჯარაში და შემდეგ მასზე განათავსონ “pop-up” ფანჯარა. თუ გვერდი ამრიგად გაიხსნება, ნამდვილი ვებ–გვერდის სამისამართო ველი ვებ–გვერდის ფონზე გამოჩნდება, თუმცა “pop-up” ფანჯარაში თქვენს მიერ შეყვანილი ნებისმიერი ინფორმაცია თაღლითების ხელში ჩავარდება, რომლებიც მას საკუთარი მიზნებისთვის გამოიყენებენ.

ინტერნეტ ბანკინგის ანგარიშში შესასვლელად, ახალ ფანჯარაში მისამართი თავად აკრიფეთ. ინტერნეტ ბანკინგის ნამდვილი ვებ–გვერდის მისამართი დაიწყება ასოებით “https”, ხოლო ბრაუზერის ფანჯრის ზედა ნაწილში პატარა "ბოქლომი" გამოჩნდება.

შეტყობინება საეჭვო წერილების მიღების შესახებ

თუ ელექტრონული ფოსტით რაიმე საეჭვო წერილს მიიღებთ, დაუყოვნებლივ შეატყობინეთ "პროკრედიტ ბანკს" უახლოეს ფილიალში მისვლით, თქვენს კლიენტთა მრჩეველთან დაკავშირებით ან შემდეგ ტელეფონის ნომერზე დარეკვით: (832) 2202222. შეგიძლიათ ასევე გადააგზავნოთ საეჭვო შეტყობინება შემდეგ საფოსტო მისამართზე: infosec@procreditbank.ge

გახსოვდეთ, რომ:

- ბანკი არასდროს მოგთხოვთ თქვენი პაროლის ან სხვა პირადი ინფორმაციის "დადასტურებას" ან "განახლებას" ბმულზე დაწკაპუნებით და ვებ–გვერდზე გადასვლის მეშვეობით. პაროლის განახლებას "პროკრედიტ ბანკი" მოგთხოვთ მხოლოდ იმის შემდეგ, რაც "პროკრედიტ ბანკის" ელექტრონული საბანკო მომსახურების საიტზე შეხვალთ, სადაც უსაფრთხო კავშირის სიმბოლო ჩანს.
- სიფრთხილე გამოიჩინეთ უცნობ ელექტრონულ წერილებთან მიმართებაში, არ გახსნათ წერილებში მითითებული ბმულები და არ შეიყვანოთ პირადი ინფორმაცია.
- ინტერნეტ ბანკინგში შესასვლელად, გახსენით თქვენი ვებ ბრაუზერი და თავად შეყვანეთ მისამართი.
- თუ შეტყობინების ნამდვილობასთან დაკავშირებით რაიმე ეჭვი გაგაჩნიათ, ან თუ ფიქრობთ, რომ თქვენ კონფიდენციალური ინფორმაცია გაამჟღავნეთ, დაუყოვნებლივ მიმართეთ "პროკრედიტ ბანკს" უახლოეს ფილიალში მისვლით, თქვენს კლიენტთა მრჩეველთან დაკავშირებით ან შემდეგ ტელეფონის ნომერზე დარეკვით: (832) 2202222. ასევე შეგიძლიათ საეჭვო შეტყობინება გადააგზავნოთ შემდეგ საფოსტო მისამართზე: infosec@procreditbank.ge

შეხსენება:

- სიფრთხილე გამოიჩინეთ უცნობი გამგზავნისაგან მოსულ წერილებთან მიმართებაში, არ ჩამოტვირთოთ და არ გახსნათ ამ წერილებში მითითებული უცნობი ვებ–გვერდების ბმულები.
- დააყენეთ და გაანახლეთ ანტი–ვირუსი, რეგულარულად შეამოწმეთ კომპიუტერი შესაძლო ვირუსების არსებობაზე.
- დააყენეთ და ისწავლეთ Firewall-ის გამოყენება.
- დააყენეთ უახლესი უსაფრთხოების განახლება, რომელიც პატჩის (patches) სახელითაა ცნობილი.